

PAPER • OPEN ACCESS

The automated networks and regional users: risk analysis of their reactions to the attacks of different destructive orientation

To cite this article: A Eshchenko *et al* 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* **537** 052020

View the [article online](#) for updates and enhancements.



IOP | ebooks™

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the [collection](#) - download the first chapter of every title for free.

The automated networks and regional users: risk analysis of their reactions to the attacks of different destructive orientation

A Eshchenko, G Ostapenko, I Bataronov and N Tolstykh

Voronezh State Technical University, Moscow ave., 14, Voronezh, 394026, Russia

E-mail: alexandra.eschencko@yandex.ru

Abstract. In work manifestations of an information war in the context of attacks to the automated networks by means of malicious codes and destructive contents are considered. Special attention is paid to users of the social automated networks which are final subject to these attacks. In this regard, authors offer a series of analytical expressions, the considering capacities of a great number of users with a different reaction to destructive content. At sufficient community of the offered technique, the emphasis is placed on the regional aspect. In particular, it is offered by polling to investigate regional resources for the purpose of forecasting of dangerous actions of their users induced by the content of different destructive orientation. All this in total forms risk model which can form a methodical basis for decision-making on counteraction of the attacks of the automated networks by means of destructive content.

1. Introduction

Mankind is in a status of world information war whereas the attacks information codes and destructive contents as which delivery system the Internet acts are used. The malicious code is aimed at gadgets, and destructive content – at human consciousness. At the same time, indifference from analogs, destruction of a subject to the attack is not provided and implements interception of management of it. It should be noted what has this appearance of the attacks rather high performance, in view of low cost and mass character of its production, a width of an area of its distribution.

In the above-stated information war, there are no rules of the game so far [1-4]. Therefore, often each state should protect independently the interests in the information sphere. It demonstrates to high unpredictability of actions of conflicting parties.

In this situation, the special importance is gained by the systems of protection against the above-stated attacks. From the information attacks, each country wishes to have such "umbrella" today. To some extent, an example of it is the People's Republic of China which information space is protected by the most powerful filter "Gold Board". Besides, in this space, the following information resources are blocked: YouTube, Instagram, Facebook, and others.

On the basis of the above, it is possible to predict a surge in the innovation activity in the creation and implementation of means of counteraction to destructive contents. Such means will bring economic and social effect in the conditions of the accruing information confrontation.



At the same time, appropriate to pay attention to a crucial role of regional aspect as the motley mentality of territorial subjects of the Russian Federation (over 100 nationalities, 11 time zones and 8 climatic zones) turns to attempt to solve the above-stated problem only at the federal level.

From here the research [5-8] of resources of the automated networks, including social orientation [9-15] regarding ensuring their safety, first of all regarding modeling of users and risk analysis of their solutions is represented relevant.

2. Risk modeling of users

A final object of destructive impacts on automated networks is their users. If to speak about the social automated networks, then the information distributed in them inducing to actions, dangerous to society, which is called often the destructive content (DC) acts as means of such influence. The involvement of users into DC, their reaction to its contents and mass character of this phenomenon define the degree of danger of the information attack.

In this regard, the research of a great number of users depending on their relation to DC is of real theoretical and practical interest. It will allow estimating analytically risks of the illegal acts induced by DC, to predict succession of events and to provide counteraction measures. Initial in this case the data which are in open access on viewings, likes, reposts and comments of user's act. From this it is obviously possible to define the corresponding areas and, therefore, to calculate damages caused to social and information space by a distribution of DC.

For a formulation of the corresponding technique, we will address to figure 1 classifying users in relation to the analyzed destructive content.

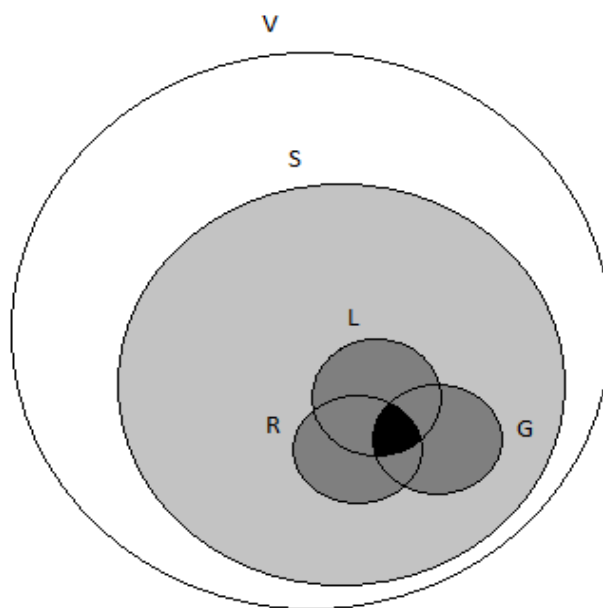


Figure 1. Euler's circles.

Euler's circles illustrating areas of the involvement of users of a resource of social networks into the process of response to distribution to them of destructive content where:

V – a great number of users of a resource;

S – a set of the browsed DC of users;

L – a set of the "liked" DC of users;

R – a great number of the users who made a report of DC;

G – a great number of the users who approved DC in the comments.

From figure 1 in relation to DC it is possible to select the following areas of users:

- a) low involvement: $A_{LI} = \frac{S}{RULUS}$;
- b) average involvement: $A_{MI} = RULUS$;
- c) high involvement: $A_{HI} = R \cap L \cap S$.

Generally, their forming, obviously, a personification of reactions of users to DC should lie.

Follows from figure 1 that the specific damage (rated by the number of users) will be for areas:

- a) low involvement

$$W_{LI} = \frac{(|S| - |A_{LI}|)}{|V|} = \frac{|S \setminus A_{LI}|}{|V|}; \quad (1)$$

- b) average involvement

$$W_{MI} = \frac{(|A_{LI}| - |A_{HI}|)}{|V|} = \frac{|A_{LI} \setminus A_{HI}|}{|V|}; \quad (2)$$

- c) high involvement

$$W_{HI} = \frac{|A_{HI}|}{|V|}. \quad (3)$$

Let's designate the probability of implementation of not virtual destructive illegal acts for areas:

- a) low involvement P_{ALI} ;
- b) average involvement P_{AMI} ;
- c) high involvement P_{AHI} .

Often [6-12], these probabilities are established by an expert way and depend on time, the virality of content and mentality of an area. The coincidence of posts of DC and aspirations of users is higher, then it is more than the value of these probabilities. Most often the ratio takes place: $P_{AHI} > P_{AMI} > P_{ALI}$.

The risk of the involvement of users of a resource into not virtual destructive activity (as for mutually exclusive areas) will be equal:

$$RiskI = W_{LI}(t)P_{ALI}(t) + W_{MI}(t)P_{AMI}(t) + W_{HI}(t)P_{HI}(t). \quad (4)$$

The last expression opens broad lands for multiple analysis and subsequent optimization. Here parameters of damage of W_{LI} , W_{MI} и W_{HI} are calculated during monitoring of the process of distribution of DC.

3. Probabilistic assessment

Above-mentioned probabilities can be also calculated on the basis of the sociological survey conducted in regional Internet resources by means of the questionnaire provided in table 1.

Shares of variously reacting users in relation to the total power of a resource, network, regional Internet space allow evaluating the expected frequency of not virtual destructive actions. Even by means of expression (1), it is possible to build rice model of information space networks of the region. It is necessary to pay attention to temporary dependence of parameters in the model (1). It means that their regular updating is necessary both during content distribution and in dynamics of development of preferences and aspirations of users of regional resources (on the basis of systematic anonymous polls

which can be held in electronic form). For this reason, the draft of the questionnaire (table 1) is offered in so laconic look.

Table 1. The draft of the questionnaire for assessment of the probability of illegal acts of users under the influence of destructive content.

Questions	Variants of answers
On what social networks did you most often face about destructive content?	<ul style="list-style-type: none"> - Facebook; - YouTube; - Vkonakte; - Instagram; - Odnoklassniki; - Twitter.
To what actions did destructive content on social networks most often provoke you?	<ul style="list-style-type: none"> - terrorism support; - incitement of hatred, hostility because of religious, ethnic and other discord; - undermining social stability; - undermining political stability; - promotion of violation of territorial integrity of the state; - the motivation of children to a commission of the actions posing threats of their life and (or) to health; - promotion of drugs, the psychotropic and stupefying substances, tobacco products, alcoholic products, gamblings, prostitution, vagrancy; - justification or justification of validity of violence and (or) cruelty; - denial of family values, disrespect of parents; - promotion of social dissoluteness; - commission of penal acts; - dissemination of the data breaking the state or other specially protected by the law secret.
What feelings are caused most often at you by destructive content of social networks?	<ul style="list-style-type: none"> - feeling of indifference; - suspicion that authors of content try to use you in the mercenary purposes; - desire to be present at protest actions on subject of content; - intention to publicly speak in favor for content; - desire to support supporters of content financially
How most often do you react on social networks to destructive content?	<ul style="list-style-type: none"> - I try not to penetrate into its contents; - I am limited to viewing; - I do likes; - I do repost; - I do comments; - I do likes, reposts, and comments at the same time

4. Conclusion

Malicious codes are generally oriented to critical objects and authorities' federal of value. In turn, the attacks like "destructive content" are in many respects aimed at regional space which in this case require special attention in terms of its protection. Monitoring of this space is of interest to researchers not only concerning diffusion [9-12] and identification of DC [13-16] but also in respect of creation regional risk models of the above-stated processes what the present article is devoted to.

Its practical sense seems that a real opportunity on the basis of reactions of users to DC appeared, taking into account probabilistic assessment of opportunities of the not virtual dangerous actions provoked by DC to receive estimates of information risks concerning the attacked regional

information space. And this procedure has an automation perspective within a software and hardware complex of monitoring of the above-stated space.

References

- [1] Radko N M, Ostapenko A G, Mashin S V, Ostapenko O A and Avdeev A S 2014 Peak risk assessing the process of information epidemics expansion *Biosciences biotechnology research* **11** 251-5
- [2] Boccatti S, Latora V, Moreno Y, Chavez M and Hwang D-U 2006 Complex networks: Structure and dynamics *Physics Reports* **424** 175–308
- [3] Tague P, Nabar S, James A R and Poovendran R 2011 Jamming-aware traffic allocation for multiple-path routing using portfolio *IEEE/ICM Transactions on networking* **19(1)**
- [4] Ahn Y, Han S, Knak H, Moon S and Jeong H 2007 Analysis of topological characteristics of huge online social networking services *16th International conference on the World Wide Web* **844**
- [5] Newman M E and Girvan M J 2004 Finding and evaluating community structure in networks *Physical Review E* **69** 58
- [6] Parinov A V, Shvartskopf E A, Popova L G, Bataronov I L and Tolstykh N N 2018 Risk models of destructive content diffusion between social network communities *International Journal of Pure Applied Mathematics* **19(15)** 605-9
- [7] Pitolin A V, Preobrazhenskiy Y P and Choporov O N 2018 Study of the possibilities of using steganographic methods of information protection *Modeling, optimization and information technologies* **(6)2** 336–53
- [8] Kravets O Ja and Choporov O N 2018 The Problems and Peculiarities of Modelling Integrated Systems of Heterogeneous Traffic Services *Journal of Siberian Federal University - Mathematics & Physics* **11** 581–7
- [9] Tsaregorodtsev A V, Kravets O Ja, Choporov O N and Zelenina A N 2018 Information Security Risk Estimation for Cloud Infrastructure *International Journal on Information Technologies and Security* **10(4)** 67–76
- [10] Parinov A V, Shvartskopf E A, Zarubin V S, Zariaev A V and Barannikov N I 2018 Risk-simulation of processes of distribution of destructive content on social network taking into account its growth *International Journal of Pure Applied Mathematics* **119(15)** 2633-7
- [11] Parinov A V, Shvartskopf E A, Parinova L V, Razinkin K A and Belonozhkin V I 2018 Social Information Networks: Models of Internetwork Malicious Content Diffusion *International Journal of Pure Applied Mathematics* **19(15)** 2639-43
- [12] Shvartskopf E A, Zariaev A V, Parinova L V and Popova L G 2016 Modeling of layering growth virus epidemic and spread of harmful content on Poisson networks *Research Journal of Pharmaceutical, Biological and Chemical Sciences* **7(4)** 2321-31
- [13] Sokolova E S, Barannikov N I, Bataronov I L and Belonozhkin V I (2016) Algorithm of Generation of Scale-Free Network at Realization Virus Attacks on Model Chiang Lu *Research Journal of Pharmaceutical, Biological and Chemical Sciences* **7(4)** 2438-47
- [14] Parinov A V, Sokolova E S, Kalashnikov A O, Tikhomirov N M and Chapurin E Y 2018 Risks of multinetwork world order and monitoring of social networks regarding detection of destructive content *International Journal of Pure and Applied Mathematics* **119(15)** 2587-91
- [15] Parinov A V, Sokolova E S, Urasov V G, Tolstykh N N and Filatov V V 2018 Destructive content in multinetwork socio-informative space: formalization of the procedure of detection *International Journal of Pure and Applied Mathematics* **119(15)** 22651-5
- [16] Romansky R (2017) A Survey of Digital World Opportunities and Challenges for User's Privacy *International Journal on Information Technologies and Security* **4(9)** 97-112